ANDREA TOGNI

Privacy as a Kantian-Misesian a priori condition for the preservation of property rights

Journal of Libertarian Studies

Togni, Andrea. 2024. "Privacy as a Kantian-Misesian a Priori Condition for the Preservation of Property Rights." *Journal of Libertarian Studies* 28 (1): 18–36. https://doi.org/10.35297/001c.116327.

ARTICLES

Privacy as a Kantian-Misesian a priori condition for the preservation of property rights

Andrea Togni[a]

Keywords: privacy, libertarianism, utilitarianism, Tornado Cash, Privacy Pools, financial regulations, crypto currencies

https://doi.org/10.35297/001c.116327

Journal of Libertarian Studies

Vol. 28, Issue 1, 2024

This article analyzes the relation between the philosophical notion of privacy, its practical implementation in the domain of cryptocurrencies, and the Western regulatory financial environment. A libertarian (anarchocapitalist, agorist) perspective is adopted. The main question concerns what kind of notion privacy is. Utilitarianism, privacy as a natural right, and privacy as a Kantian-Misesian a priori condition for the preservation of property rights are analyzed. First, it is shown that utilitarian approaches do not work because they let the government define privacy, thus corrupting its practical implementation. The cases of Tornado Cash and of Privacy Pools, two privacy-preserving cryptocurrency protocols, are discussed to prove the point. Second, the theory of privacy as a natural right is discarded because it is not compatible with libertarian reductionism. Third, the main proposal of this article is to define privacy as a Kantian-Misesian a priori condition for the preservation of property. This proposal is coherent with libertarian reductionism because privacy is not understood as a natural right; moreover, it is superior to utilitarianism because the a priori status of privacy protects it from the arbitrary wishes of politicians and bureaucrats. The origin of a priori notions is not empirical, but their use is: privacy cannot but impact how the acting man protects real-world property and interacts with fellow human beings.

The Tornado Cash saga and Privacy Pools

The ability of governments to extract resources from the economy depends on their ability to surveil it: property that is not seen by authorities cannot be taxed (Togni 2022a, 2022b). Cryptocurrencies pose a special danger to the state because they are not issued by central banks, because they can be used globally without asking for permission from regulators, and because some implement privacy features that make surveillance extremely challenging.

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CCBY-4.0). View this license's legal deed at http://creativecommons.org/licenses/by/4.0 and legal code at http://creativecommons.org/licenses/by/4.0/legalcode for more information.

a Andrea Togni (andrea.togni@protonmail.com) is an independent researcher currently working on privacy. He is also a high-school teacher of history and philosophy. In 2018, he earned a PhD in the philosophy of mind with a dissertation on the criteria for individuating the senses.

Nontraceable money allows buyers and sellers to interact without relying on regulated financial institutions, thus bolstering black (free) markets and hindering tax collection.[1] It comes as no surprise, then, that governments are cracking down on privacy-centric crypto projects. The worldwide clampdown on Tornado Cash (TC), a privacy opt-in tool developed for the Ethereum blockchain, is used here to exemplify the point. The first section of this article focuses on the technical and regulatory sides of the TC saga; broader philosophical implications will be discussed in the second half.[2]

OFAC versus Tornado Cash

The Office of Foreign Asset Control (OFAC) is part of the United States Treasury Department; its role is to administer and enforce "economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States." OFAC publishes the Specially Designated Nationals and Blocked Persons (SDN) List, which is "a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific." Sanctioned entities' assets are frozen and all US citizens are forbidden from interacting with them. In August 2022, OFAC (2022) added some TC smart-contract addresses to the SDN list. TC is a set of smart contracts on the Ethereum blockchain through which users can deposit their coins, receive a zero-knowledge proof of deposit, and withdraw the same coins to a different account, thus regaining pseudonymity.[3] (Wade, Lewellen, and Valkenburgh 2022; Valkenburgh 2022). OFAC sanctioned TC because its smart contracts have been used by hacker organizations like the Lazarus Group, which is tied to the North Korean government.

OFAC's announcement of sanctions against TC shows how government regulations can be used as attack vectors against the adoption of privacy-preserving crypto tools. First, the title of the press release calls TC a mixer, but this is inaccurate because "users can only withdraw the specific tokens they originally deposited" (Wade, Lewellen, and Valkenburgh 2022), meaning that no one's coins are ever mixed with others' coins at any point of the

1 Black, nonregulated markets are free in the sense that economic actors can escape state violence. Of course, some participants may engage in violent activities, but this is also true for legal, regulated markets.

2 Attacks on privacy come from both public and private actors. Given that governments are the most powerful entities on earth and that prominent private-sector privacy violators like Big Tech companies only exercise "governmentality" (Rectenwald 2019), this article deals mainly with aggressions originating from the state; still, the principles discussed here can be applied to attacks perpetrated on a smaller scale.

3 Usually, cryptocurrencies are pseudonymous by default: on-chain activities are available for everyone to see but are not directly related to a real-world person. Pseudonymity is the most basic privacy protection for cryptocurrencies, but it is lost, for example, when users hand over Know Your Customer (KYC) information to third parties such as exchanges. TC and other opt-in privacy tools help users regain pseudonymity.

process. Second, OFAC draws a misleading parallel between TC and Blender.io. Blender.io is a centralized mixing service that was sanctioned by OFAC because of its role in laundering profits for darknet marketplaces like Hydra (OXT Research 2022). But TC has no centralized operator; on the contrary, "a user who deposits and later withdraws tokens maintains total ownership and control over their tokens, even as they pass through the pool. At no point is the user required to relinquish control of their tokens to anyone" (Wade, Lewellen, and Valkenburgh 2022). In other words, while Blender.io is a centralized, custodial service, the core of TC is decentralized and noncustodial.[4] Third, OFAC (2022) complains that "Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks." But it is technically impossible to impose such controls: TC, unlike banks and regulated crypto exchanges, is a truly decentralized service that functions deterministically. TC addresses and software "are widely distributed tools, ideas fixed in a shared medium of expression (the Ethereum blockchain), copies of which exist on the personal computers of thousands of persons around the world. Additionally, the small minority of contracts listed by OFAC that retain some level of human updateability are not actually used to control, mix, or move user funds. They are either ancillary services, donation addresses for software development efforts, or defunct and now unused contracts on the Ethereum blockchain" (Valkenburgh 2022). Given that no human being or entity controls the TC pools used to gain pseudonymity, it is hard to understand who would be responsible for the controls demanded by the US government. Fourthly, OFAC (2022) complains that TC "indiscriminately facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin." But TC does not facilitate transactions on its own: users facilitate their own transactions and maintain full control of their funds at every step of the process. Fifthly, a consequence of sanctions is that "all property and interests in property of the entity above, Tornado Cash, that is in the United States or in the possession or control of U.S. persons is blocked and must be reported to OFAC." Again, TC is not an entity but software that users can run on their devices without asking for permission from anyone. Moreover, TC property cannot be blocked, because it is not an entity that can own property. What the OFAC enforcement actions block is the ability of common users to interact with TC smart contracts to protect the privacy of their finances. TC developers also created a compliance tool that can be used to demonstrate the origin and legitimacy of one's funds; in other words, OFAC prevents law-abiding citizens from safeguarding their pseudonymity online while proving their compliance to

4 TC is a *set* of smart contracts. The contracts governing the pools that are used to anonymize funds function deterministically, meaning that they execute rules automatically, outside the control of any human being, developers included. Other addresses, like the ones used to receive donations or to provide relaying services, retain some level of human control, but this does not affect the functioning of the pools.

US law. Last, OFAC's stance affects regulators and law enforcement's actions worldwide. A few days after OFAC updated its SDN list, Dutch authorities arrested Alexey Pertsev, a TC developer, for money laundering (FIOD 2022).[5] The arrest of Pertsev sets a dangerous precedent: the fact that he wrote part of the TC code does not imply that he himself laundered money through TC. Unfortunately, the obvious distinction between people who write software that anyone can use autonomously and criminals does not seem to be obvious to some zealous prosecutors.

The Indictment of Roman Semenov and Roman Storm

In August 2023, Roman Semenov and Roman Storm, two lead TC developers, were indicted by the US Attorney's Office for the Southern District of New York for operating an unlicensed money-transmitting business, for money laundering, and for violating international sanctions imposed by the US government (United States v. Storm and Semenov (S.D.N.Y. 2023)).

The negative bias against privacy projects emerges clearly from the arguments adopted by the US attorney. Some commentators (Valkenburgh 2023; Gruenstein, Norris, and Barabander 2023) note that the indictment goes against the guidance of the Financial Crimes Enforcement Network (FinCEN 2019) on money transmission, which distinguishes between anonymizing software and anonymizing services. Given that TC is noncustodial, it falls under the first category, meaning that it should not be required to register as a money transmission service or to comply with anti-money-laundering legislation. Still, the indictment alleges that TC is a centralized service, and not just software, because of Semenov and Storm's control over the TC web user interface. While this last point is correct, the US attorney fails to see that having control over a website is not the same as having control over smart contracts, controlling users' funds, and transmitting money on behalf of clients. Moreover, the indictment does not account for sophisticated hackers such as the Lazarus Group likely being able to interact with TC smart contracts directly, without the help of a user interface.[6]

Another point exploited by the US attorney is that the TC governance system makes use of a decentralized autonomous organization (DAO) and the TORN token. However, the indictment does not explain how the DAO works or how controlling the DAO implies controlling the money deposited in TC pools. In fact, the DAO cannot influence the functioning of TC pools or users' behavior. Moreover, while it is true that Semenov and Storm

5 At the date of writing, Pertsev is still in custody in the Netherlands. He was indicted for laundering $1.2 billion on March 27, 2024; the verdict will be delivered on May 14, 2024.

6 In general, the user interface is not a necessary piece of TC: everyone can interact with the smart contracts directly.

allocated a significant number of TORN tokens to themselves and profited from the role of TORN in the TC ecosystem and that TORN is probably an unregistered security, it is also true that users enjoy total control over their funds regardless of the role of these tokens.[7] In other words, making profits from an unregistered security is not necessarily the same as transmitting money on behalf of others and should not in itself be considered money laundering.

The indictment also complains that Semenov and Storm shared tips with TC users to help them protect their anonymity and safety. For example, using Tor or a VPN while interacting with a financial service is recommended because it obscures the relation between one's financial activity and one's IP address. Another recommendation is to never reuse a cryptocurrency address to prevent external observers from correlating one's on-chain activities. While this and other advice from Semenov and Storm is correct and helpful, privacy-conscious users are a nuisance from a law enforcement perspective because it is not easy to surveil them. Changing cryptocurrency addresses, for example, weakens the effectiveness of OFAC sanctions. Given that the SDN list targets specific addresses, sending funds to an address with no sanctions against it is a pretty straightforward strategy to evade them; unfortunately for the US attorney, attacking commonsense privacy advice does not make OFAC methodology sound.

The TC saga is constitutionally relevant. The Fourth Amendment, for example, does not protect the right of law enforcement agencies to surveil citizens, but it does protect a citizen's right to financial privacy and personal security. By attacking TC and not the criminals who use TC, the US government is depriving law-abiding citizens of an effective tool to safeguard their constitutionally protected right to privacy. Moreover, it can be argued that the TC developers' right to freedom of expression is being threatened despite its constitutional protection under the First Amendment. The indictment complains multiple times that Semenov and Storm did not implement Know Your Customer (KYC) guidelines in the TC software. Anti-money-laundering procedures require regulated intermediaries to collect personal data about their clients to prevent and tackle money laundering. The idea is that clients pose risks to the stability of the financial system and that they should be surveilled by default even when there is no evidence of criminal behavior. Pressuring developers into implementing KYC guidelines in their software is deeply problematic. First, writing code is not the same as running a regulated financial entity: confusing these two activities, as the indictment repeatedly does, is a grave misconception. Second, cryptocurrencies and crypto tools are just lines of code, which are constitutionally protected speech. The crypto wars of the 1990s resulted in

7 TORN tokens are used to pay fees and to express voting rights in the DAO.

judiciary wins for privacy activists and debased the argument that the state can force developers to implement weak encryption that can be circumvented by law enforcement (Epstein 2020). In other words, developers are free to write whatever code they like and to not incorporate the US government's "suggestions" into their work. Defending freedom of speech is not the same as endorsing crime: verbal and written speech is constitutionally protected even if it can be used to order a hit man to commit a homicide; similarly, code is constitutionally protected even if it can be used for nefarious purposes. Speech and code are not crimes in themselves but expressions of human nature. Like the crypto wars, the TC saga shows that the US government is willfully trying to obfuscate the difference between writing code, on the one hand, and committing and inciting crime, on the other.

Privacy Pools

One possible answer to the regulatory crackdown on privacy-preserving crypto projects is to try appeasing regulators. In September 2023, the Privacy Pools (PPs) protocol was proposed by some big names in the cryptocurrency ecosystem to address both users' demand for privacy and the concerns of US regulators who attacked TC (Buterin et al. 2023). According to the authors,

> the core idea of Privacy Pools is this: instead of merely zero-knowledge-proving that [users'] withdrawal is linked to some previously-made deposit [like in TC], a user proves membership in a more restrictive association set. The association set could be the full subset of previously made deposits, a set consisting only of the user's own deposit, or anything in between . . . instead of requiring the user to specify exactly which deposit their withdrawal came from, or on the other extreme providing no information at all beyond a proof of nondouble-spending, we let the user provide a set of possible origins of their funds, and this set can be as wide or as narrow as they wish.

PPs are designed to incentivize users to associate only with other "low-risk" participants and to exclude "high-risk" depositors from their association sets; this way, the financial history of cryptocurrency users would not be in plain sight for everyone to see, thus protecting privacy, and bad actors would not be able to hide in the crowd, thus fostering regulatory compliance.[8] But who decides who is a good actor and who is not? Not the individual user: "In practice, users will not be manually picking and choosing deposits to include in their association set. Rather, users will subscribe to intermediaries that we can call association set providers (ASPs), which generate association sets that

8 In transparent blockchains such as Bitcoin and Ethereum, all transactions are visible by default to external observers. By entering an association set, users break the deterministic link between deposit and withdrawal, making it impossible for external observers (everyone but the user herself) to track funds. However, association sets can be built so that "illicit funds" are prevented from entering them and enjoying their privacy benefits.

have certain properties." ASPs are centralized entities that can be pressured into enforcing many common practices of the financial industry that are antithetical to the preservation of privacy.[9] ASPs may require users to provide a proof-of-personhood, such as government-backed ID, before joining their association set; users may be required to verify their identity with mechanisms similar to the ones used by social media; ASPs may take advantage of AI-based scoring systems that evaluate the risk profile of every user who interacts with an association set; a bank may restrict its association set to customers who have undergone KYC verification; and so on. Because of this flexibility, proponents of PPs argue that their approach lets everyone have her cake and eat it too: users can hide in association sets composed of a significant number of people, while regulators can ensure that those association sets are compliant with national legislation. PPs are meant to adapt to different regulatory environments with their own criteria to form association sets and exclude bad actors. Moreover, cryptocurrency users "could issue a membership proof against the intersection of [multiple] association sets and thereby credibly demonstrate that the deposit corresponding to their withdrawal is in line with the requirements of [multiple] jurisdictions." In short, the main objective of PPs is to make peace between privacy activists and regulators: "In many cases, privacy and regulatory compliance are perceived as incompatible. This article suggests that this does not necessarily have to be the case, if the privacy-enhancing protocol enables its users to prove certain properties regarding the origin of their funds."

While the PPs proposal is technically innovative and interesting, it is not immune to economic and philosophical shortcomings. For example, because it is an opt-in privacy protocol that can be added on top of transparent blockchains, users' privacy is not protected by default. This is problematic because privacy by default is one of the main tools for the protection of property rights (Togni 2022a, 2022b). The lack of privacy protections by default implies that fungibility gets hurt. In the case of money, fungibility is the ability of a coin to be interchanged with another similar coin. But the availability of different pools creates a system of tiered association sets, some of which are more accepted than others. Consequently, monetary units A and B, which should have the same value, may be valued differently in reality because only one of the two is accepted in this or that association set. Moreover, the prices of coins in a pool may differ from the prices of coins that never touched one. In general, from a monetary perspective, being able to interact in many different ways with different association sets is a bug, not a feature, because it means that different behaviors can be observed by external watchers, who can exploit this information to the detriment of users.

9 The very existence of ASPs threatens decentralization, which is one of the key promises of cryptocurrencies.

Buterin et alii praise the ability of PPs to foster freedom of disassociation from bad actors.[10] By letting users choose who they want to associate with, dangerous terrorists and criminal organizations can be isolated and prevented from enjoying privacy protections, thus making the world a better place. This sounds great in theory, but reality tells another story. Freedom of disassociation is not a necessary feature of money, as gold and silver demonstrate. Gold and silver coins do not tell the history of their owners by default; this implies that present holders do not need to worry about disassociation from previous ones. From a monetary perspective, this is a feature, not a bug, because money is first and foremost a medium of exchange, not a tool to attack bad actors; precious metals can be exchanged seamlessly by everyone without the need to investigate the history of every single coin. The ability to use money as a political tool against political enemies is an "innovation" of the fiat system; not coincidentally, the use of financial sanctions against nonaligned countries has skyrocketed in recent years. Freedom of disassociation gets easily transmuted into forced disassociation and blackmail: whoever does not comply with the latest sanctions issued by three-letter agencies is threatened with grave consequences, as seen in the case of TC. The decision to classify an entity as good or bad is arbitrary and often serves the purposes of powerful Western governments, which are inclined to exploit their control over the financial system to hit geopolitical adversaries and perceived enemies. When proponents of PPs argue for freedom of disassociation, they argue for something very similar to the state-dominated and hyper-surveilled fiat system and for something very different from traditional money favorable to freedom, such as gold and silver coins.

Some private entities are set to earn a lot of money by becoming ASPs. The most obvious candidates are blockchain surveillance (BS) companies, which are private firms that sell their services to regulated entities and law enforcement agencies (Togni 2023). BS firms profit from developing closed-source software that flags "suspicious" activity on public blockchains. On-chain activities can be considered "suspicious" even when they are perfectly legal, such as transactions linked to privacy add-ons or withdrawals from a crypto ATM. The fact that BS software is closed-source is highly problematic because nobody can verify the assumptions that are used to flag "suspicious" activity; in other words, what counts as "suspicious" is decided arbitrarily by these companies. BS firms use heuristic rules to discriminate between "good" and "bad" transactions. Importantly, heuristic rules are just educated guesses that are then used in court to restrict people's liberty.[11] The following

10 PPs are presented as a privacy tool. But privacy involves the individual, while freedom of disassociation is a social, collective construct. Conflating individual and social interests confuses the proposal.

11 Even the most basic transaction on a transparent blockchain can be interpreted in many ways. To flag a transaction as "suspicious," BS firms have to make assumptions, which may or may not turn out to be accurate. The fact that educated guessing is being used more and more in Western courts is highly problematic.

declaration to a district court by Elizabeth Bisbee (United States v. Sterlingov (D.D.C. 2023)), head of investigations at Chainalysis, one of the biggest BS firms, is revealing: "Chainalysis clustering methodologies have not been peer-reviewed in the sense that an academic paper would get peer-reviewed with data and methodology(ies) reviewed in a separate study by other scientists. However, every single clustering heuristic in the system has been reviewed by numerous Chainalysis data scientists, intelligence analysts, and investigators that specialize in blockchain analytics." Not only does Bisbee ask the court to just trust BS "scientists" who were not able (or willing) to get their work peer-reviewed, but she also admits that "Chainalysis has not gathered and recorded in a central location false positives/false negatives because there is design to be more conservative in the clustering of addresses. In response to the Court's inquiry, Chainalysis is looking into the potential of trying to collect and record any potential false positives and margin of error, but such a collection does not currently exist." It cannot be stressed enough that "evidence" from BS companies is being used in courts to restrict people's liberty. The fact that one of the authors of the PPs paper works for Chainalysis is a massive red flag for any serious privacy activist.

The most important promise of PPs may be their ability to create a neutral financial environment where jurisdictions and actors can set rules according to their particular needs. But PPs' overall approach is relativistic, not neutral. Never in the paper is the term "privacy" defined; on the contrary, the authors make it very clear that they are happy to accept whatever definition is provided by government agencies. This mixture of relativism and the authority principle creates a fundamental asymmetry that heavily favors regulators and cronies, such as are found in BS firms, and heavily penalizes ordinary people, thus making PPs anything but neutral. A financial system is neutral if it can be used by everyone without asking for permission from authorities; that is, true neutrality requires that even the most committed enemy cannot be prevented from interacting with that system. Gold and silver coins and physical fiat cash come close to this ideal, which explains why they are under constant regulatory attack and why governments relentlessly nudge people to use electronic fiat money through regulated intermediaries. A non-financial example of actual neutrality is the Continental, a hotel chain from the *John Wick* film series. These hotels accommodate criminals from different organizations, but violence against other guests is strictly prohibited on hotel property and incurs harsh punishment.[12] Similarly, a neutral financial system must prevent powerful governments from exploiting their territorial monopoly on legal violence against their enemies. To achieve this goal, the definition of privacy cannot be left in the hands of partisan

12 Not coincidentally, guests pay for their stay in gold coins.

politicians and bureaucrats but must be established on independent philosophical grounds, which is precisely what proponents of PPs refuse to do.

The Philosophical Notion of Privacy

The cryptocurrency ecosystem interests philosophers who deal with privacy and money because of its experimental nature and because it does not completely capture free-market forces. Privacy-preserving digital money is kryptonite to the state. If widely adopted, governments will not be able to control economic activity as pervasively as they do now. This would significantly harm the effectiveness of tax collection and therefore put their very survival in danger. The crackdown on TC and other privacy-centric crypto projects is not surprising: the aggressiveness of three-letter agencies does not depend on their willingness to fight crime but on their willingness to fight financial instruments that threaten the state's monopoly on money. Cryptocurrency players who want to foster actual freedom must adopt the adversarial mindset that, sooner or later, regulators will try to push them out of existence. Developing the ability to survive on black (free) markets is their only chance. Thriving on black markets requires both a competent technical implementation and a sound understanding of the philosophy of privacy. The following pages will focus on the philosophical side of the issue. The main question is about what kind of notion privacy is. Utilitarianism, privacy as a natural right, and privacy as a Kantian-Misesian a priori condition for the preservation of property rights are analyzed. The discussion is framed by the domain of money and cryptocurrencies, but it concerns other domains as well.

The Inevitable Failure of Utilitarianism

Utilitarians view privacy as a spectrum and in terms of costs and benefits: maximum privacy protects honest users but also criminals, while maximum transparency may harm innocent citizens but is good for law enforcement and for fighting crime. Proponents of PPs tend to advocate for something in the middle: on the one hand, innocent crypto users should be afforded some degree of privacy; on the other hand, law enforcement should be afforded some degree of insight into financial transactions. One problem with this approach is that it does not account for inequality among participants in the cryptocurrency ecosystem. Regulators and private-sector cronies, having more political and economic power than ordinary individuals, can make their own analyses of costs and benefits seem more important. Authors of PPs present their work as an attempt to find a "practical equilibrium" between privacy and regulation, but this "equilibrium" cannot but heavily skew in favor of the powerful. De facto, the public is blackmailed into entering association sets that are approved by regulators. If the "wrong" association set is chosen, grave legal consequences may follow.

Utilitarians face crucial questions: What prevents the government from demanding more transparency, by mandating, for example, that every participant in every association set undergo a full KYC review? What prevents the state from imposing not only blacklists but also whitelists? What prevents governments from prohibiting any association set with more than one member? If the balance between privacy and transparency is only a matter of costs and benefits, then the state can claim that mass surveillance prevents crime and that citizens who have nothing to hide have nothing to fear. For the government, the power that comes with mass surveillance outweighs the privacy lost by ordinary citizens. The most that utilitarians can do is hope the government does not abuse its power and accepts a reasonable compromise.

Utilitarianism is often praised as a pragmatic philosophy that avoids the shortcomings of more rigid and uncompromising approaches. But it only works when the parties negotiating the compromise do so in good faith and aim for a good outcome for everyone. As the TC saga shows, this ideal is complicated by privacy, money, and state power. The government, for example, claims that it needs mass surveillance to prevent crimes such as money laundering. It is estimated that up to $2 trillion are laundered worldwide per year; Chainalysis reports that "mixers [like TC] processed a total of $7.8 billion in 2022, 24 percent of which came from illicit addresses, whereas in 2021, they processed $11.5 billion, only 10 percent of which came from illicit addresses. The data suggests that legitimate users have decreased their use of mixers, possibly due to law enforcement actions against prominent ones, while criminals have continued to use them" (Chainalysis 2023, 46). Even Chainalysis admits that regulations hurt law-abiding citizens more than criminals. The practical result of law enforcement actions is that ordinary people are afraid to use effective tools like TC to protect their financial privacy, while criminals continue to experiment with cutting-edge solutions. Moreover, in 2022, mixers like TC were used to launder less than $2 billion, or 0.001 percent of money laundered worldwide; in contrast, "mainstream centralized exchanges were the biggest recipient of illicit cryptocurrency, taking in just under half of all funds sent from illicit addresses" (Chainalysis 2023, 43), or around $12 billion. In other words, regulated cryptocurrency exchanges were used to launder six times the amount of illicit money that went through privacy-preserving tools like TC. In addition, the vast majority of the $2 trillion money-laundering business goes through traditional fiat institutions. Governments are aware of this data, but it does not prevent them from practicing mass surveillance. The primary objective of these practices is not to fight crime[13] but to surveil the population and gain more control. The assumption that regulators act in

13 From a utilitarian perspective, the government can argue that, even if mass surveillance practices allow to tackle only a small percentage of crime, the benefits are bigger than tackling no crime at all. Utilitarian privacy activists cannot really rebut this kind of argument because the government, not them, decides what is useful and what is not.

good faith when it comes to privacy-preserving crypto tools is naïve at best, but utilitarians, like proponents of PPs, ignore this issue and continue to seek a "practical equilibrium" with state agencies. The only practical outcome, however, will be more power for regulators and less privacy for ordinary users.

The utilitarian thesis that privacy is a spectrum fails to distinguish the practical aspect of privacy from the theoretical one. Practically speaking, individuals can protect their privacy by, for example, using curtains to make their apartments more private or using cash instead of credit cards. PPs, too, can help safeguard privacy in some cases. But from a theoretical perspective, the notion of privacy is more rigorously defined and, even if it is violated constantly, cannot be debased. Utilitarians, however, avoid theoretical notions of privacy and instead outsource its definition to the government, thus corrupting its practical implementation.

Privacy as a Kantian-Misesian A Priori Condition for the Preservation of Property Rights

Libertarians and privacy activists need a strong theoretical notion of privacy that does not depend on empirical circumstances or the arbitrary choices of politicians and bureaucrats. Equipped with a strong theoretical notion, they can focus on implementing privacy in money and other domains and deploy a real-world strategy to foster liberty and hinder violence. In Togni (2022a, 2022b), privacy is understood as the condition of being invisible by default to enemies and visible by choice to trusted peers. Despite articulating this definition, Togni does not explain what kind of theoretical notion privacy is.

The theory that privacy is a natural right suggests that it is absolute—that is, not subject to human arbitrariness. But this approach runs against libertarian reductionism, which holds that only property is a natural right and that every other right can be reduced to it. Libertarian reductionism can be applied successfully to the domain of information in general and of financial information in particular. Given that information longs to be free and that the human mind is the exclusive property of the individual, it is illegitimate to punish people for sharing their thoughts. In other words, people can think and speak as they please without needing permission. No right to privacy can surpass property rights over one's own body and mind. The same holds true for public information about cryptocurrency transactions: public ledgers are available for everyone to see and public data can be exploited against cryptocurrency holders. In the domain of information and money, privacy is not a right but a *fight*: financial information, such as private keys, must be continuously protected from potential adversaries. For example, private keys that allow to spend cryptocurrencies must be kept private at all times, otherwise funds will be lost. Moreover, it is highly recommended to use nontransparent cryptocurrencies that hide the sender of a transaction, its recipient, and the amount spent: making this information public does not lead to a loss of funds but may allow would-be thieves to deanonymize users

and therefore to attack them, even physically. The more that information remains under the exclusive control of the individual, the more that money can be defended from the assaults of private and public adversaries.

However, privacy is not only a real-world fight. This article proposes to define privacy as a Kantian-Misesian a priori condition for the preservation of property rights; this theoretical understanding of privacy makes the practical fight purposeful.[14] Kant is the founder of transcendental philosophy: "I apply the term transcendental to all knowledge which is not so much occupied with objects as with the mode of our cognition of these objects, so far as this mode of cognition is possible a priori" (Kant 1855). The purpose of transcendentalism is to find the a priori (universal and necessary) conditions of human knowledge. The intellect, according to Kant, is regulated by a priori categories, such as the pure concept of causality, which allows human beings to explain reality in terms of causes and effects. The origin of the concept of causality is not empirical; rather, it is a universal and necessary mental category that every person cannot but deploy to understand the world. Mises applies the Kantian method to praxeology and to the science of economics. The thesis that "human action is purposeful behavior" (Mises 1998, 11) is the a priori truth from which all other truths about the acting individual can be derived.

Mises proposes the following test to ascertain whether a proposition is a priori or not:

> If we qualify a concept or a proposition as a priori, we want to say: first, that the negation of what it asserts is unthinkable for the human mind and appears to it as nonsense; secondly, that this a priori concept or proposition is necessarily implied in our mental approach to all the problems concerned, i.e., in our thinking and acting concerning these problems. The a priori categories are the mental equipment by dint of which man is able to think and to experience and thus to acquire knowledge. Their truth or validity cannot be proved or refuted as can those of a posteriori propositions, because they are precisely the instrument that enables us to distinguish what is true or valid from what is not. (Mises 2006, 15)

In what follows, Mises's test is applied to the notion of privacy. In Togni (2022a), privacy is defined as "the ability to make property invisible by default to enemies and visible by choice to trusted peers." Privacy and property

14 Togni (2022b) argues that privacy is a condition of the *existence* of property in the domain of information and a condition of its *defense* in the physical domain. When the term "preservation" is used in these pages, it is meant to encompass both realms in a neutral way.

behave differently in the physical domain and in the realm of information (Togni 2022b).[15] This article uses physical money and cryptocurrencies as its primary case studies.

First, in the domain of digital and mental information, privacy is a condition of the existence of property in the sense that exclusive ownership of information can be maintained if and only if nobody but the owner can see it (Togni 2022b). This is an a priori truth: it is unthinkable that information could be public and at the same time the exclusive property of an individual. Enjoying exclusive property rights to an idea is the same as keeping it completely private. As soon as it is shared with someone else, it enters her mind and becomes her idea so that exclusive ownership is lost. Similarly, owning cryptocurrencies is the same as keeping the private keys private. As soon as the private keys are leaked, one's wallet can and will be emptied by external observers. While in the domain of information privacy is all or nothing, in the physical domain there are degrees of visibility and invisibility because of the nature of material bodies. In both cases, privacy is an a priori condition for the preservation of property. It is unthinkable, for example, to maintain exclusive property of a gold bar without maintaining at least some degree of privacy. Let's say that A places her gold bar in the middle of Piazza del Duomo in Milan unguarded and available for everyone to see. Given that people are not morally perfect, on a long enough timeline that gold bar will be taken by someone despite A's legitimate property claim. If A decides to leave her gold bar in Piazza del Duomo under the protection of a guard, the gold bar is no longer completely visible and undefended. Still, on a long enough timeline, the gold bar will be stolen by someone better armed or more astute than A's guard. If property is valuable, adversaries will invest in resources to take it. An effective defense of physical private property is unthinkable in the absence of some significant degree of invisibility. Both in the physical and in the digital domain, the more privacy is protected, the better property is preserved. While the practical implementation of privacy is an empirical issue, its necessity to safeguard property is an a priori truth.

Second, a proposition is a priori if it "is necessarily implied in our mental approach to all the problems concerned, i.e., in our thinking and acting concerning these problems." Privacy satisfies this requirement with regard to the preservation of property. Cryptocurrency owners, for example, must find ways to keep private keys invisible by default to potential enemies. Dependable wallets, multisignature schemes, and safe physical storage are possible solutions. Similarly, the owner of a gold bar cannot but develop some strategy to hide it from potential thieves. Outsourcing its security to trusted custodians and using a personal safe-deposit box are just two among many possible solutions. Dealing with property inevitably leads to developing

15 For simplicity, property rights of the body and of the mind are not discussed in this paper.

strategies to make it invisible by default to potential enemies and visible by choice only to trusted peers. Such strategies need not be conscious attempts to implement explicit theories, but they are always at least implicit in the behaviors of those who want to preserve their property (e.g., in the use of doors to protect houses or the decision to share the location of a safe only with trusted family members). Whether or not a strategy is effective is an empirical issue; that there must exist an implicit or explicit privacy-focused strategy to preserve property is an a priori truth.

Third, the "truth or validity [of a priori propositions] cannot be proved or refuted as can those of a posteriori propositions, because they are precisely the instrument that enables us to distinguish what is true or valid from what is not." The empirical fact that slavery exists does not disprove the existence of natural property rights of the body; the empirical fact that people make bad decisions does not disprove the truth that every human action aims at replacing an unsatisfactory state with a more satisfactory one; the fact that privacy is often violated in the real world does not imply that it is an empirical notion; and the fact that regulators try to impose arbitrary definitions of privacy does not imply that it must be understood in utilitarian terms. According to Kant, a priori concepts cannot be proven or refuted empirically, but their *use* is always empirical. The a priori notion of privacy makes it possible for people to defend tangible property, creators to understand what it means to own ideas, cryptocurrency holders to preserve their wealth, and people to protect property rights and interact peacefully with others.

The contrast between the utilitarian and the Kantian-Misesian approaches could not be more stark. Utilitarians believe that privacy is just a matter of costs and benefits; however, in the real world, regulators define what these are. Kantians and Misesians, on the other hand, know that privacy cannot be arbitrarily defined by the powerful, because it is a universal requirement for the actual implementation of natural property rights. The government, for example, argues that taxation is legitimate, because the common good is superior to the individual good, and that tax avoidance, which relies on excellent privacy practices, is a social cost too large to tolerate. Utilitarians cannot rebut this line of reasoning but only try to convince the government to moderate its efforts toward taxation and against privacy. Principled libertarians, however, know that theft is a crime against natural property rights, even when it is committed by the powerful, and try to develop real-world strategies to hide their possessions to avoid being robbed by government agents. Utilitarians, like proponents of PPs, do not object to the legitimacy of US sanctions, but principled libertarians will maintain that an Iranian who wants to send money to a North Korean should be able to do so without hassle. Utilitarians develop tools such as PPs that allow Western governments to censor cryptocurrency transactions they do not like, while principled libertarians develop crypto tools that help the Iranian and the North Korean protect themselves from the prying eyes of government

snitches. More generally, utilitarians try to appease the government and to push the argument that cryptocurrencies should be permitted on legal markets. Kantians and Misesians, however, know that asking for permission is asking for denial; therefore, they create parallel societies and black markets where cryptocurrencies are used regardless of what politicians think.

Privacy as an a priori condition for the preservation of property comes with its own costs. Timothy May, one of the most prominent figures in the cypherpunk movement, which inspired the birth of cryptocurrencies, is not afraid to face them: "The state will of course try to slow or halt the spread of this [privacy-preserving] technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy" (May 1992). Privacy is truly neutral, meaning that both honest people and bad actors (individual criminals and private and public criminal organizations) can take advantage of it. Nobody can stop this from happening. Privacy is not arbitrarily defined by the state or by utilitarians; rather, it is an a priori condition that shapes all human behaviors. The theory that mass surveillance and compliance will halt crime is empirically false and does not account for human nature. Governments and utilitarians pushing for this flawed theory will only diminish the privacy of law-abiding individuals, give more power to the state, and maintain the privacy of criminals.[16] Privacy is not a moral category or a political notion but a human category. PPs code and US government legislation will not change human nature. The question is not how to stop criminals from using privacy-preserving technology but how good people can leverage their natural tendency to privacy so that natural property rights are preserved effectively.

Conclusion

The TC saga is just one of many cases in which Western governments have cracked down on privacy tools that threaten their monopoly on money and their ability to surveil citizens. TC and PPs are relevant from technical and policy perspectives as well as for different philosophical understandings of privacy. The central claims of this article are that (1) utilitarian approaches cannot foster actual liberty, because they lack an independent theory of privacy and accept whatever definition the government provides, and (2), in the Kantian-Misesian approach, the a priori notion of privacy is coherent with human nature and with natural property rights.

16 It can be argued that the more privacy is criminalized, the more criminals are incentivized to test and adopt extreme solutions and thus *increase* their privacy.

Submitted: December 09, 2023 CST. Accepted: February 26, 2024 CST. Published: April 19, 2024 CST.

REFERENCES

Buterin, Vitalik, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani. 2023. "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium." Working paper, Social Science Research Network, September 9, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364.

Chainalysis. 2023. *The 2023 Crypto Crime Report*. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.

Epstein, Jim. 2020. "When Encryption Was a Crime: The 1990s Battle for Free Speech in Software." *Reason*, October 21, 2020. https://reason.com/video/2020/10/21/cryptowars-gilmore-zimmermann-cryptography/.

FinCEN. 2019. *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies.* May 9, 2019. https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

FIOD. 2022. "Arrest of Suspected Developer of Tornado Cash." August 12, 2022. https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/.

Gruenstein, Benjamin, Evan Norris, and Daniel Barabander. 2023. "Secret Notes and Anonymous Coins: Examining FinCEN's 2019 Guidance on Money Transmitters in the Context of the Tornado Cash Indictment." Working paper, International Academy of Financial Crime Litigators, September 2023. https://www.cravath.com/a/web/szBQs6mB8ewbTKqHi2XnaY/86m4BH/1693580906839.pdf.

Kant, Immanuel. 1855. *The Critique of Pure Reason*. Translated by J. M. D. Meiklejohn. London.

May, Timothy. 1992. "The Crypto Anarchist Manifesto." Presented at the Cypherpunks gathering in Silicon Valley, Calif., November 21. https://activism.net/cypherpunk/crypto-anarchy.html.

Mises, Ludwig von. 1998. *Human Action: A Treatise on Economics*. Scholar's ed. Auburn, Ala.: Mises Institute. https://mises.org/library/human-action-0.

———. 2006. *The Ultimate Foundation of Economic Science: An Essay on Method*. Edited by Bettina Bien Greaves. Indianapolis, Ind.: Liberty Fund. https://oll.libertyfund.org/titles/greaves-the-ultimate-foundation-of-economic-science-an-essay-on-method.

OFAC (Office of Foreign Asset Control). 2022. "US Treasury Sanction Notorious Virtual Currency Mixer Tornado Cash." Press release. August 8, 2022. https://home.treasury.gov/news/press-releases/jy0916.

OXT Research. 2022. "The Fall of Hydra Market." October 13, 2022. https://www.oxtresearch.com/the-fall-of-hydra-market/.

Rectenwald, Michael. 2019. *Google Archipelago: The Digital Gulag and the Simulation of Freedom*. Nashville, Tenn.: New English Review Press.

Togni, Andrea. 2022a. "Privacy as Invisibility (by Default): Bridging the Gap between Anarcho-Capitalists and Cypherpunks." *Journal of Libertarian Studies* 26 (1): 1–23. https://jls.mises.org/article/57657-privacy-as-invisibility-by-default-bridging-the-gap-between-anarcho-capitalists-and-cypherpunks.

———. 2022b. "The War on Privacy—or, Privacy as a Strategy for Liberty." *Rivista italiana di filosofia politica*, no. 3, 243–59. https://doi.org/10.36253/rifp-2025.

———. 2023. "The Government Wants to Turn Blockchain Firms into Servants of the State." *Mises Wire*, July 28, 2023. https://mises.org/wire/government-wants-turn-blockchain-firms-servants-state.

Valkenburgh, Peter van. 2022. "How Does Tornado Cash Actually Work?" Coin Center. August 25, 2022. https://coincenter.substack.com/p/how-does-tornado-cash-actually-work.

———. 2023. "New Tornado Cash Indictments Seem to Run Counter to FinCEN Guidance." Coin Center. August 23, 2023. https://www.coincenter.org/new-tornado-cash-indictments-seem-to-run-counter-to-fincen-guidance/.

Wade, Alex, Michael Lewellen, and Peter van Valkenburgh. 2022. "How Does Tornado Cash Work?" Coin Center. August 25, 2022. https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/.